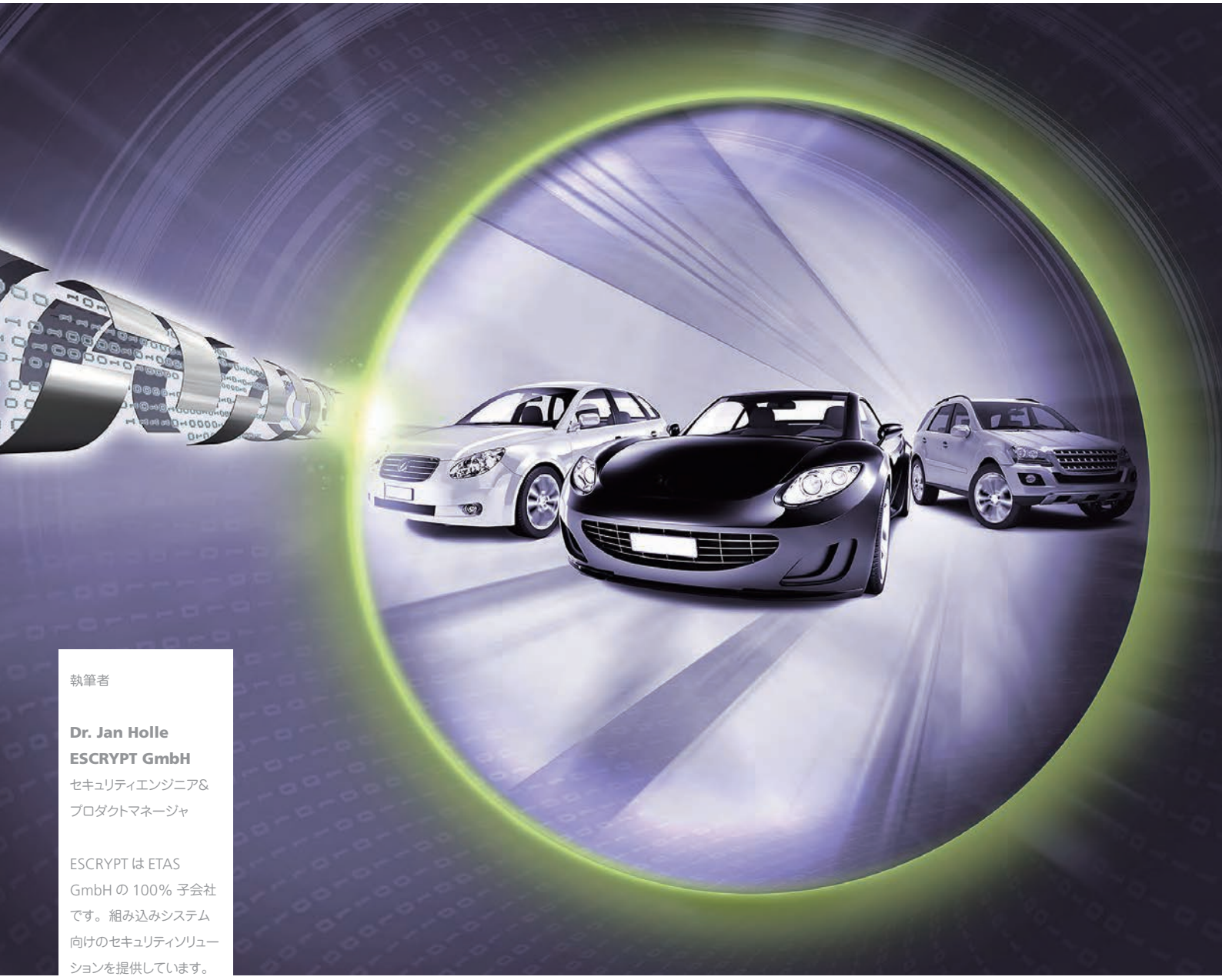
Immune System for the Connected Vehicle

コネクテッドビークルの免疫システム



執筆者

Dr. Jan Holle
ESCRYPT GmbH
セキュリティエンジニア&
プロダクトマネージャ

ESCRYPT は ETAS GmbH の 100% 子会社です。組み込みシステム向けのセキュリティソリューションを提供しています。

侵入検知・防御システム（IDPS: Intrusion detection and prevention system）

安全性と快適性が高まり、サービスが最適化され、車の運転をより楽しめる。コネクテッドビークルには多くの長所があります。しかし、「モノのインターネット（IoT）」に組み込まれることにはリスクも伴います。IoT ではサイバー攻撃の危険が増大し、悪用できそうな新たな脆弱性を攻撃者たちが絶えず探し求めています。そのため、コネクテッドビークルには、未知のパターンの攻撃さえも検知して、新しい攻撃パターンをネットワーク上の他のコネクテッドビークルに迅速に伝えることのできる、学習型の防御システムが必要です。

車両が一度お客様に所有されると、メーカーはその車両システムに時折アクセスする程度になります。しかし、それでも購入者は自分の車両がいつも保護されていることを当然のこととして期待します。車両が続々とコネクテッド化される中で、新たな問題も持ち上がっています。IoT に組み込まれると、確かにメーカーが車両にアクセスできる可能性は高まることになりますが、それと同時に車両が不正アクセスや悪意のあるサイバー攻撃を受けるリスクも高まってしまいます。もはや機能安全だけでは不十分です。世界中の道路を何億台ものコネクテッドビークルが走行することになるのであれば、メーカーは包括的な自動車 IT セキュリティも保証しなければなりません。これに加えて、私たちは今後の自動運転の動向も考慮しなければならないため、IT システムの安全性とセキュリティに関する要求がますます増えることになります。

ライフサイクル全体にわたる包括的防御

要求されるセキュリティレベルを実現する前提として、十分に考え抜かれた方策が効果的に実施されなければなりません。自動車のセキュリティは後付けできません。少なくとも莫大なコストをかけなければ不可能です。それに代わる方策として、開発の開始から安全性とセキュリティを考慮していくという全体論的な戦略が必要になります。このソリューションには、信頼できる防御策など、組み込みソフトウェアの開発段階で標準化されるプロセスも含まれます。ハードウェアセキュリティモジュールやセキュアハードウェアエクステンションを含む、ハードウェアセキュリティアドオンを使用する現代のチップアーキテクチャは、安全関連のシステムドメインを不正アクセスから物理的に保護します。これらのセキュリティコアの周りにはさらに、ECU ファームウェアのマニピュレーションを認識するセキュアブート機能や、すべての通信を保護するための保護ネットワークゲートウェイまたは暗号ソリューションなどの方策が必要です。同じく重要なのは、セキュリティエリアへのアクセスを制限することや、暗号鍵およびロック解除コードのアクセス権を責任能力のある数名の個人だけに与えること、開発・製造段階における組織的な防御策です。

上述の方策は、偶発的なエラーの可能性を下げ、ハッカーによる車載システム侵入の試みを阻止します。しかし、これらの方策だけでは、お客様の所有物となった車両のコネクテッドシステムの防御をどのようにして保証するかという問題の解決にはなりません。ライフサイクルの中段階にもなると、メーカーは限られた機会しか車両にアクセスすることができません。理屈の上では、今後 10 年以上にわたる攻撃に対処できるように、メーカーが開発段階のうちに車両システムに対策を施しておくことが必要ということになります。しかし、10 年前の情報技術の状況を振り返ってみても、そのようなことは到底不可能であることがわかるはずです。

課題：未知の危険に対する防御

論理的結論としては、車両がお客様に所有されていても、そのシステムを確実に防御するために、IT セキュリティ対策は動的でしかも継続的なものでなければなりません。ただし、機能安全の境界条件は主として自然法則や統計的予測に基づいていて、車両の使用段階でもそのまま適用されることになりますが、IT セキュリティの仮定と境界条件は不安定で変わりやすいものです。攻撃者はシステムの新たなウィークポイントを絶えず探し求めていますが、メーカーはこれらのウィークポイントの存在にそもそも気付いていない場合がほとんどです。一方、セキュリティ専門家も、今後何年もの間に出現する可能性のあるすべての攻撃戦略を予知することはできません。既存の IT も、未知のパターンを用いた攻撃から IT インフラストラクチャを防御するという難題に直面しています。この場合も、攻撃者は完全な防御を実現するように考え抜かれたセキュリティメカニズムを回避しようとします。この分野では次第に、「防御」とはすなわち「インテリジェントな侵入検知・防御システム（IDPS）を整備すること」を意味するようになりつつあります。さらによく注目すると、IDPS は、コネクテッドビークルの保護にも最適なシステムであることがわかります。

IDPS による予防措置

IDPS テクノロジーならではの強みは、車両の接続性を使用することによって新しい攻撃シナリオに素早く反応することができ、さらにその防御戦略をすぐに車両フリート全体に伝えることができることです。これにより、攻撃に対して動的に反応する一種の免疫システムが構築され、その免疫システムの下では新たな攻撃が発見されるたびにフリートの防御力が強化されていきます。

ESCRYPT の IDPS の中核となっているのは、ECU やゲートウェイを監視して車載ネットワークの電気通信全体を絶えず分析し続ける特別なセキュリティソフトウェアです。異常が発生すると、このソフトウェアはそれを記録し、さらに、深刻な脅威が存在する場合は防御策を推進します。検知された攻撃パターンが既知のものである場合は、ファイアウォールメカニズムが各種データバス間の通信をブロックします。これはすでに日常的な流れであり、IDPS 全体と同様に、将来のイーサネットネットワークだけでなく、今日の主流である CAN のネットワークでも使用することができます。

しかし、IDPS テクノロジーの真価は、未知のパターンと攻撃戦略を認識して撃退できることにあります。これを行うために、IDPS はルールセット（ブラックリストとホワイトリスト）を複数個保有して、その内容は絶えず更新されています。このアプローチの強みの 1 つとして、異常や未知の攻撃の手がかりは“CycurIDS”という攻撃認識ソフトウェアによって検知されますが、このソフトウェアは、異常に関する情報を後で見直せるように車両に保存しておくことができます。そして、さらに効果的なのは、すべての異常に関する情報をクラウドベースのイベントデータベースに自動送信する機能です。イベントデータベースには、同じメーカーのすべてのコネクテッドピークルから送信されたすべての異常に関する情報を、既知の攻撃者の履歴情報と一緒に格納するので、分析時にはそれらを効果的に比較することができます。

フリート全体に対する動的防御戦略の構築

データの分析から、OEM はハッカーがどのような戦略を遂行していてどのウィークポイントを標的にしているか、そして特定の領域に攻撃が集中しているかどうかという点について、常に最新の

包括的概観情報を受け取ります。この包括的なイベントデータベースをバックエンドで評価するために、動的防御システムの次の段階として、ビッグデータを自動分析する CycurGUARD ソフトウェアソリューションが稼働します。このソフトウェアは攻撃パターンを分析して事前分類処理を実行します。それに基づいて、サイバーディフェンスセンターのセキュリティアナリストと犯罪科学スペシャリストが、対抗措置が必要かどうか、および必要な場合はどの対抗措置を開始するべきかを決定します。その措置としては、ファイアウォールの調整や、CycurIDS ルールセットの更新、また影響を受ける ECU のソフトウェアに内在する脆弱性を ECU メーカーとの緊密な協議に基づいて取り除くことなどが考えられます。こうした措置は無線通信で、フリート内のすべてのコネクテッドビークルに、もちろん暗号化によって保護され伝えられます。さらに、更新情報は気付かないうちに第三者によって変更されることのないように、デジタル署名で保護されます。

まとめ

ネットワーク上のすべての車両で検知されたすべての異常に関する情報が、中心となるクラウドベースのイベントデータベースに集められるので、新しい攻撃パターンは即座に識別されます。新たな車両がこのネットワークに接続されるたびに、IDPS はますますインテリジェントになり、脅威に対してより的確な防御策を装備できるようになります。なぜなら、これまで見ることのできなかった攻撃（たとえば、ファイアウォールによってブロックされていた攻撃など）が継続的な状況評価の対象として送り込まれてくるようになり、以前よりも迅速かつ的確に最新のリスクに的を絞ってセキュリティ対策を適合させることができるようになったからです。この結果、ネットワーク内にはコネクテッドビークル用の免疫システムが構築されます。この免疫システムは新しい攻撃が企てられるたびに強化され、さらに優れた防御を実現していきます。データベースは絶えず拡大を続けている上、防御戦略をフリート内のすべての車両に素早く伝えるので、これまで以上に包括的なオールラウンドの防御を常に確実に行えるようになります。

予防処置済みフリートへの
5 ステップ